
- Lab Overview & Needed Software
- Installing Kali as a virtual Machine
- Basic Overview of Kali Linux
- The Terminal & Linux Commands
- Python 2 VS Python 3 & Writing Our First Program
- Installing & Using a Python IDE
2. Writing a Mac Address Changer - Python Basics

- What is MAC Address & How To Change it
- Using Python Modules & Executing System Commands
- Implementing a Very Basic MAC Changer
- Variables & Strings
- Using Variables in MAC Changer
- Getting Input From The User
- Handling User Input
- Handling Command-line Arguments
- Initialising Variables Based on Command-line Arguments
Functions

Returning Values From Functions

Decision Making – Theory

Using Conditional Statements in MAC Changer
3. Mac Changer - Algorithm Design

- Extracting a Substring Using Regex
- Regular Expressions (Regex)
- Refactoring & Housekeeping
- Implementing The Algorithm to Check The Mac Did Change
4. Programming a Network Scanner

- Programming a Network Scanner
- Installing Windows as a Virtual Machine
- What is ARP & What it's Used For?
- Designing an Algorithm To Discover Clients Connected To The Same Network
- Using Scapy To Create an ARP Request
- Combining Frames To Broadcast Packets
- Sending & Receiving Packets
- Lists
- Iterating Over Lists & Analysing Packet
● Using Escape Characters To Enhance Program Output
● Dictionaries
● Improving the Program Using a List of Dictionaries
● Iterating Over Nested Data Structures
● Get IP Range Using Command Line Arguments
● Python 3 Compatibility
5. Writing An Arp Spoofer

- What is ARP Spoofing?
- Redirecting the Flow of Packets in a Network Using arpspoof
- Sending ARP Responses
- Extracting MAC Address From Responses
- Loops
- More on Loops & Counters
- Dynamic Printing
- Handling Exceptions
- Implementing a Restore Function
- Restoring ARP Tables When an Exception Occurs
6. Writing a Packet Sniffer

- Sniffing Packets Using Scapy
- Extracting data From a Specific Layer
- Analysing Sniffed Packets & Extracting Fields From Layers
- Analysing Fields & Extracting Passwords
- Extracting URLs
- Capturing Passwords From Any Computer Connected to the Same Network
8. Writing a File Interceptor

- Filtering Traffic Based on the Port Used
- Analysing HTTP Requests
- Intercepting HTTP Requests
- Modifying HTTP Responses on The Fly
- Intercepting & Replacing Downloads on The Network
9. Writing a Code Injector

- Analysing HTTP Responses
- Replacing a Substring Using Regex
- Decoding HTTP Responses
- Modifying HTTP Responses & Injecting Javascript Code in HTML Pages
- Debugging Issues Using Groups & None-capturing Regex
- Recalculating Content Length
- BeEF Overview & Basic Hook Method
- Hooking Computers Using code_injector
- Basic BeEF Commands
- Delivering Malware Using BeEF
10. Bypassing HTTPS

- How to Bypass HTTPS
- Bypassing HTTPS & Sniffing Login Credentials
- Replacing Downloads on HTTPS Pages
- Injecting Code in HTTPS Pages
11. Writing an ARP Spoof Detector

- Running Python Programs on Windows
- Capturing & Analysing ARP Responses
- Detecting ARP Spoofing Attacks
12. Writing Malware

- Execute System Command Payload
- Filtering Command Output Using Regex
- Stealing WiFi Passwords Saved on a Computer
- Downloading Files From Program
- Writing Files on Disk
- Password Recovery Basics
- Using all the Above to Steal Saved Passwords Remotely
- Interacting With The File System
13. Writing Malware - Keylogger

- Writing a Basic Local Keylogger
- Logging Special Keys
- Global Variables
- Threading & Recursion
- OOP - Object Oriented Programming Basics
- Constructor Methods & Instance Variables
- Constructor Methods & Instance Variables
14. Writing Malware - Backdoor

- Troubleshoot device access control
- Client - Server Communication & Connection Types
- Connecting Two Remote Computers Using Sockets
- Sending & Receiving Data Over TCP
- Executing System Commands Remotely
- Implementing a Server
- Implementing Skeleton For Server - Client Communication
- Refactoring - Creating a Listener Class
- Refactoring - Creating a Backdoor Class
- Serialisation – Theory
- Serialisation - Implementing Reliable Methods to Send & Receive Data Over TCP
- Serialisation - Reliably Sending & Receiving Data
- Sending Commands as List & Implementing Exit Command
- Interacting With the File System - Implementing "cd" Command
- Reading Files
- Writing Files
- Downloading Files From Hacked Computer
- Implementing Upload Functionality in Listener
- Implementing Upload Functionality in Backdoor
- Handling Unknown Exceptions
- Using the Backdoor to Hack Windows, Linux & OS X
15. Writing Malware - Packaging

- Converting Python Programs To Windows Binary Executables
- Running Executables Silently
- Installing Windows Pyinstaller on Linux
- Packaging Programs For Windows From Linux
- Persistence Idea
- Running Programs on Startup
- Creating a Basic Trojan Using Download & Execute Payload
- Creating a Trojan By Embedding Files In Program Code
- Bypassing Anti-Virus Programs – Theory
- Bypassing Anti-Virus Programs – Practical
- Adding an Icon to Generated Executables
- Spoofing File Extension
- Converting Python Programs to Linux Executables
- Converting Python Programs To OS X Executables
16. Website / Web Application Hacking

- What is a Website
- How to Hack a Website
17. Website Hacking - Writing a Crawler

- Sending GET Requests To Web Servers
- Discovering Subdomains
- Discovering Hidden Paths in Websites
- Reading Response Content
- Extracting Useful Data From Response
- Filtering Results
- Extracting Unique Links & Storing Them In a List
- Recursively Discovering All Paths On a Target Website
18. Writing a Program to Guess Login Information

- Sending Post Requests to Websites
- Guessing Login Information on Login Pages
19. Writing a Vulnerability Scanner

- Parsing HTML Code
- Posting Forms
- Building Basic Structure For Vulnerability Scanner
- Using Default Parameters
- Sending Requests in a Session
- Extracting & Submitting Forms Automatically
- Implementing a Method To Run The Scanner
- Discovering XSS Vulnerabilities
- Exploiting XSS Vulnerabilities
- Implementing Code To Discover XSS in Forms
- Implementing Code To Discover XSS in Parameters
- Automatically Discovering Vulnerabilities Using the Vulnerability Scanner
Questions?

We would like to hear from you

0803 7084 968

0803 0887 945

@loctechng

@loctech

@loctechtraining

No. 4A Etim Okpoyo Close, By Linjo Super Market, Bridge Bus-Stop, Aba Express Road, Port Harcourt, Rivers State